

## CLAIMS

1. A system for enhancing security of end user station access to  
5 Internet and intranet(s), e.g. of corporate access, over access  
network access points, comprising gateway packet data nodes  
(3A,3B), packet data support nodes (2;2,2'),  
c h a r a c t e r i z e d i n  
that it comprises security indication providing means (11; 12; 13;  
10 11A, 11B; 12A, 12B; 13A, 13B) for providing an (corporate) access  
point with a security criterium indication (defining security) and  
for distributing said security indication to a packet data support  
node (2;2,2'), and in that a security enforcement mechanism  
(21;21<sub>1</sub>,21A;21B) is provided in the packet data support node  
15 (2;2,2'), said security enforcement mechanism at least providing  
for preventing all other traffic not fulfilling the security  
criterium conflicting the security indicated access point when  
there is a connection requiring security over the security  
indicated access point, at least until the last packet of the  
20 security indicated access point connection has been sent.

2. A system according to claim 1,  
c h a r a c t e r i z e d i n  
that the security criterium indication comprises a security  
25 marking indicating that the access point supports the provision of  
secure access point connections.

3. A system according to claim 1,  
c h a r a c t e r i z e d i n  
30 that the security criterium indication comprises an indication as  
to the criterium/criteria that is/are to be fulfilled for  
concurrent conflicting access point connections in order for them

to be allowed simultaneously with a first secure access point connection.

4. A system according to claim 2 or 3,

5 characterized in  
that the security criterium/criteria indication comprises a flag,  
an attribute or a data structure.

5. A system according to any one of the preceding claims,

10 characterized in  
that the security indicating and distributing means are provided  
in a gateway packet data node.

6. A system according to any one of the preceding claims,

15 characterized in  
that the gateway packet data node comprises a GGSN.

7. A system according to any one of claims 1-4,

20 characterized in  
that the security indicating and distributing means are provided  
in a Home Location Register (HLR).

8. A system according to any one of claims 1-4 and 6,

25 characterized in  
that the security indicating and distributing means are provided  
in a Domain Name Server (DNS).

9. A system according to any one of the preceding claims,

30 characterized in  
that the security indicating means are provided in a CGSN  
comprising the functionality of a GGSN and SGSN.

10. A system according to any one of the preceding claims,

c h a r a c t e r i z e d i n  
that an access point is security indicated through providing an  
Access Point Name (APN) thereof with the security indication, e.g.  
an attribute.

5

11. A system according to any of the preceding claims,  
c h a r a c t e r i z e d i n  
that access point connections comprise PDP contexts.

10 12. A system according to claim 11,  
c h a r a c t e r i z e d i n  
that the enforcement mechanism is dynamic, and in that in the  
packet data support node (SGSN;CGSN) means are provided for  
dropping all traffical packets of other PDP contexts not meeting  
15 the security criterium/criteria when a simultaneous PDP context to  
a security marked access point is used for communication of  
packets.

13. A system according to claim 12,  
20 c h a r a c t e r i z e d i n  
that the packet data node (SGSN, CGSN) comprises means for  
detecting traffic on a PDP context to a security indicated access  
point, and means for activating security protection and in that it  
further comprises means for, after lapse of a predetermined,  
25 configurable time period after sending of the last packet on a PDP  
context with a security indication, allowing traffic on other PDP  
contexts again.

14. A system according to any one of claims 1-11,  
30 c h a r a c t e r i z e d i n  
that the enforcement mechanism is static and in that means are  
provided in a packet data support node, e.g. SGSN or CGSN, for  
deactivating access point connections, e.g. PDP contexts, which do

not meet the security criterium/criteria when a security condition is met for one connection to a security indicated access point.

15. A system according to claim 14,

5 c h a r a c t e r i z e d i n

that a security condition is met when a request is received in the packet data support node (SGSN;CGSN) relating to activation of a PDP context to a security indicated APN.

10 16. A system according to claim 14,

c h a r a c t e r i z e d i n

that a security condition is met when a PDP context to a security marked APN has been activated in the packet data support node.

15 17. A system according to claim 14,

c h a r a c t e r i z e d i n

that a security condition is met when traffic/a packet is detected on a PDP context to a security indicated access point.

20 18. A system according to claim 16 or 17,

c h a r a c t e r i z e d i n

that the packet data support node comprises means for re-activation of deactivated PDP contexts, and in that said means e.g. are end user controlled.

25

19. A packet data support node (PDN;SGSN;CGSN) (2;2,2') for enhancing security at end user station access to Internet and intranet(s), e.g. corporate access,

c h a r a c t e r i z e d i n

30 that it comprises a security enforcement mechanism, said security enforcement mechanism comprising means for receiving and detecting an access point security indication from a security indication providing and distributing means,

traffic preventing means for preventing all other traffic not fulfilling (a) security criterium/criteria conflicting a security indicated access point connection at least until the last packet of the security indicated access point connection has been sent.

5

20. A packet data support node according to claim 19,  
c h a r a c t e r i z e d i n  
that security indication comprises a number of criteria to be fulfilled by concurrent/conflicting access point connections in  
10 order for them to be allowed simultaneously with other secure access point connections.

21. A packet data support node according to claim 19 or 20,  
c h a r a c t e r i z e d i n  
15 that the security indication comprises an Access Point Name (APN) indication.

22. A packet data support node according to claim 21,  
c h a r a c t e r i z e d i n  
20 that it comprises an SGSN.

23. A packet data support node according to claim 21,  
c h a r a c t e r i z e d i n  
that it comprises a CGSN.

25  
24. A packet data support node according to claim 22 or 23,  
c h a r a c t e r i z e d i n  
that the access point connections comprise PDP contexts.

30 25. A packet data support node according to claim 24,  
c h a r a c t e r i z e d i n

that the enforcement mechanism is dynamic, providing for dropping of all traffical packets of all PDP contexts not meeting the security criterium/criteria, but keeping the PDP contexts.

5 26. A packet data support node according to claim 25,  
c h a r a c t e r i z e d i n  
that it comprises means for detecting traffic on a PDP context to  
a security indicated access point (APN), and means for activating  
security protection and in that it further comprises means for,  
10 after lapse of a predetermined, configurable time period after  
sending of the last packet on a PDP context to a security  
indicated access point, allowing traffic on other PDP contexts.

15 27. A packet data support node according to claim 24,  
c h a r a c t e r i z e d i n  
that the enforcement mechanism is static and in that the packet  
data support node comprises means for deactivating access point  
connections, e.g. PDP contexts, which do not meet the security  
criterium/criteria when security protection is required for an  
20 access point connection (PDP context), i.e. a security protection  
condition is met.

25 28. A packet data support node according to claim 24,  
c h a r a c t e r i z e d i n  
that a security condition is met when a request is received  
relating to activation of a PDP context to a security indicated  
APN.

30 29. A pcket data support node according to claim 24,  
c h a r a c t e r i z e d i n  
that a security condition is met when a PDP context to a security  
marked APN is activated.

30. A packet data support node according to claim 29,  
c h a r a c t e r i z e d i n  
that the packet data support node comprises means for re-  
activation of deactivated PDP contexts, and in that said means are  
5 end user controlled.

31. A node in a mobile communication system supporting  
communication of packet data comprising security indicating means  
for providing access points with a security indication to allow  
10 for secure remote access connections to corporate networks,  
c h a r a c t e r i z e d i n  
that the security indicating means further comprises are  
associated with a distribution functionality such that a security  
indication can be distributed to a packet data support node  
15 (SGSN;CGSN),  
that said security indicating means support provisioning of an  
access point with a security criterium indication indicating  
which, if any, access point connections are allowed simultaneously  
over the access point.

20 32. A node according to claim 31,  
c h a r a c t e r i z e d i n  
that the security indication is provided to an Access Point Name  
of the access point.

25 33. A node according to claim 32,  
c h a r a c t e r i z e d i n  
that an access point connection comprises a PDP context and in  
that the security criterium indication comprises an indication of  
30 which criteria, if any, that have to be fulfilled by  
concurrent/conflicting access point connections in order to be  
allowed/prohibited when an access point is security indicated.

34. A node according to any one of claims 31-33,  
c h a r a c t e r i z e d i n  
that it comprises a Gateway GPRS Support Node (GGSN).

5 35. A node according to any one of claims 31-33,  
c h a r a c t e r i z e d i n  
that it comprises a Domain Name Server (DNS).

10 36. A node according to claim 35,  
c h a r a c t e r i z e d i n  
that the Domain Name Server comprises an extended functionality  
for storing IP addresses and security indications, the DNS server  
comprising dedicated or specific records for or comprising  
security indications.

15 37. A node according to any one of claims 31-33,  
c h a r a c t e r i z e d i n  
that it comprises a Home Location Register (HLR).

20 38. A method for enhancing security of end user station access to  
Internet and intranet(s), e.g. corporate access,  
c h a r a c t e r i z e d i n  
that it comprises the steps of:

- establishing if a an access point needs to be secure; if  
25 yes,
- providing the access point (identifier) with a security  
indication with one or more criteria in a network node,
- distributing the security indication to a packet data  
support node,
- 30 - enforcing the security indication by at least preventing all  
traffic on all access point connections conflicting a first  
security indicated access point connection to/through the  
security indicated access point and not fulfilling the



security criterium/criteria at least until the last packet of the security indicated access point connection has been sent.

5 39. A method according to claim 38,

c h a r a c t e r i z e d i n

that it comprises the step of:

- providing the security indication in a gateway packet data node, e.g. a GGSN, in a HLR or in a DNS.

10

40. A method according to claim 38 or 39,

c h a r a c t e r i z e d i n

that the step of providing a security indication comprises,

- providing an Access Point Name (APN) with the security indication.

15

41. A method according to claim 40,

c h a r a c t e r i z e d i n

that the access point connections comprise PDP contexts.

20

42. A method according to claim 41,

c h a r a c t e r i z e d i n

that the enforcing step comprises:

- dropping all traffical packets of all other PDP contexts than a first incoming security requiring PDP context which do not meet the security criterium/criteria.

25

43. A method according to claim 41,

c h a r a c t e r i z e d i n

that the enforcing step comprises:

- deactivating all other conflicting PDP contexts than a first security requiring PDP context, which do not fulfill the security criterium/criteria.

30